UNITED STATES DISTRICT COURT
DISTRICT OF NEW HAMPSHIRE

IN THE MATTER OF THE SEARCH OF: ONE BLUE MAXWELL BD-R 25GB BLU-RAY DISK AND ONE GEEK SQUAD THUMB DRIVE, NOW IN THE CUSTODY OF HSI MANCHESTER.	Case No. 21-mj-184-01-AJ **Filed Under Seal**

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, Ronald Morin, a Special Agent with the United States Department of Homeland Security, Immigration and Customs Enforcement, Homeland Security Investigations (HSI), being duly sworn, do depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing a search of one Maxwell BD-R 25GB blu-ray disk and one Geek Squad thumb drive ("SUBJECT DEVICES"), further described in Attachment A, for the things described in Attachment B—specifically, evidence, fruits, and instrumentalities of the foregoing criminal violations which relate to possession and access with intent to view child pornography.

2. I am a Special Agent with the Department of Homeland Security, Immigration and Customs Enforcement, Homeland Security Investigations (HSI), and have been so employed since May 2006. I am currently assigned to the Manchester, New Hampshire field office. As part of my regular duties as an agent, I investigate criminal violations relating to a broad range of immigration and customs related statutes, including those relating to child exploitation and child pornography. I have received training in the

area of child pornography and child exploitation, and as part of my duties have observed and reviewed numerous examples of child pornography (as defined in 18 U.S.C. §2256) in various forms of media, including digital/computer media. I have conducted investigations and executed search warrants involving child exploitation and child pornography offenses.

3. I am a "Federal law enforcement officer" within the meaning of Federal Rule of Criminal Procedure 41(a)(2)(C), that is, a government agent engaged in enforcing the criminal laws and duly authorized by the Attorney General to request a search warrant.

4. The statements in this affidavit are based on my own investigation of this matter as well as on information provided by other law enforcement officers. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. While I have included all material facts relevant to the requested search warrant, I have not set forth all of my knowledge about this matter.

5. I submit that the facts set forth in this affidavit establish probable cause to believe that violations of 18 U.S.C. § 2252(a)(4)(B) have been committed and that there is probable cause to believe that fruits, evidence, and instrumentalities of the Specified Federal Offenses are likely to be found in the LAPTOP, as set forth below.

SPECIFIED FEDERAL OFFENSES

6. Title 18, United States Code, Section 2252(a)(4)(B) and (b)(2) prohibit any person from knowingly possessing or accessing with the intent to view, or attempting or conspiring to possess or access with the intent to view, 1 or more books, magazines, periodicals, films, video tapes, or other matter which contain any visual depiction that has been mailed, or has been shipped or transported using any means or facility of interstate or foreign commerce or

in or affecting interstate or foreign commerce, or which was produced using materials which have been mailed or so shipped or transported, by any means including by computer, if the production of such visual depiction involved the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct.

DEFINITIONS

7. The following definitions apply to this Affidavit and Attachment B:

a) "Child pornography," as defined in 18 U.S.C. § 2256(8), is any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical or other means, of sexually explicit conduct, where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

b) "Computer," as used herein, refers to "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device" and includes smartphones, other mobile phones, and other mobile devices. See 18 U.S.C. § 1030(e)(1).

c) "Computer hardware," as used herein, consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including central processing units, internal and peripheral storage devices such as fixed disks,

external hard drives, "thumb," "jump," or "flash" drives, which are small devices that are plugged into a port on the computer, and other memory storage devices); peripheral input/output devices (including keyboards, printers, video display monitors, and related communications devices such as cables and connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including physical keys and locks).

d) "Computer passwords and data security devices," as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates what might be termed a digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

e) "Records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form.

f) A "storage medium" is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, "thumb," "jump," or "flash" drives, CD-ROMs, and other magnetic or optical media.

g) "Cloud storage," as used herein, is a form of digital data storage in which the digital data is stored on remote servers hosted by a third party (as opposed to, for example, on a user's computer or other local storage device) and is made available to users over a network,

typically the Internet.

h) The "Darknet" is an overlay network within the Internet that can only be accessed with specific software, configurations, or authorization, and often uses a unique customized communication protocol.

i) The "Tor network" or "Tor" is free and open-source software for enabling anonymous communication by directing Internet traffic through a free, worldwide, volunteer overlay network consisting of more than seven thousand relays to conceal a user's location and usage from anyone conducting network surveillance or traffic analysis. Tor is available to Internet users and is designed specifically to facilitate anonymous communication over the Internet. The Tor network attempts to do this by routing Tor user communications through a globally distributed network of relay computers, along a randomly assigned path known as a "circuit."

j) A "hidden service," also known as an "onion service," is website or other web service that is accessible only to users operating within the Tor anonymity network.

k) The "Internet" is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

l) An "Internet Protocol address" or "IP address," as used herein, refers to a unique numeric or alphanumeric string used by a computer or other digital device to access the Internet. Every computer or device accessing the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer or device may be directed properly from its source to its destination. Most Internet Service Providers ("ISPs") control a range of IP addresses. IP

addresses can be "dynamic," meaning that the ISP assigns a different unique number to a computer or device every time it accesses the Internet. IP addresses might also be "static," if an ISP assigns a user's computer a particular IP address that is used each time the computer accesses the Internet. ISPs typically maintain logs of the subscribers to whom IP addresses are assigned on particular dates and times.

m) "Minor," as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.

n) "Sexually explicit conduct," as defined in 18 U.S.C. § 2256(2), means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the anus, genitals, or pubic area of any person.

PROBABLE CAUSE

8. In February 2020, the HSI Manchester, NH, office received information that originated from a foreign law enforcement agency known to the Federal Bureau of Investigation (FBI) and with a history of providing reliable, accurate information in the past. In part, the information provided by the foreign law enforcement agency specified that on April 28, 2019, at 20:25:08 UTC, an individual originating from IP address 65.175.213.176 accessed a known Darknet web site that facilitated the sharing of child sex abuse and exploitation material with a particular emphasis on sexually explicit material depicting young boys. Users of the website were able to view some material without creating an account. However, an account was required to post and access all content.

9. According to publicly available information, IP address 176 is owned and operated by Atlantic Broadband. On or about September 9, 2019, a summons was served on Atlantic Broadband for subscriber information associated with the IP address on April 28, 2019 at 20:25:08 UTC. Atlantic Broadband provided the following subscriber details:

a. Subscriber name: Michael Clemence

b. Service and billing address: Rochester NH

c. Phone numbers: 7209, -0703

10. A query of publicly available databases for information related to Michael Clemence revealed the following: year of birth 1985; last known address: Rochester, NH. The queries also indicated that Michael Clemence is married to Elizabeth Clemence and has two young children.

11. CLEAR records identified Michael Clements' date of birth as [REDACTED]/1985, SSN [REDACTED], address ochester NH, email address @msn.com. Criminal history checks revealed no derogatory information. Property record checks indicated that he purchased the Adams Ave. property on 10/28/2019 with Elizabeth Anne Clemence.

12. On May 26, 2021, SA Mike Perella, SA Sean Serra, and SA Derek Dunn conducted a consensual knock and talk with Michael Clemence ("Clemence") at in Rochester. Clemence answered the door and agents identified themselves. SA Perella advised Clemence that agents were at his residence to ask about certain internet activity that occurred in April of 2019 at his previous residence, in Rochester. Clemence expressed

suspicion at the reason for agents' presence and advised that he had consumed a couple of beers. Clemence advised that his wife, Elizabeth, was at work.

13. During the conversation, Clemence volunteered that the tenant that lived next door to him at was an IT specialist and had done some IT work for him. Clemence identified this neighbor as "Kevin," and advised that "Kevin" had since moved to Maine. Clemence was vague about the nature of the IT work "Kevin" had done for him in the past.

14. Agents advised Clemence that they were investigating internet activity associated with child exploitation material, and that some of this activity occurred in April 2019 from the IP address associated with his previous residence on Clemence expressed vague familiarity with the dark web, offering that he understood that it was used to buy and sell illegal drugs. When asked, Clemence denied any knowledge of Tor.

15. Clemence then described an event that took place around that same time in 2019 in which his wife was looking on their laptop and she viewed something that appeared to be "really bad." Clemence relayed that his wife was very alarmed at what she saw on the computer and she did not know what it was or how it got onto the computer. Clemence did not elaborate or provide specifics about what his wife had observed on the computer. After observing this material on the computer, he and his wife "wiped" the computer and gave it to a family friend.

16. Agents asked Clemence about the computer he currently had. In response, Clements stated that he had a computer that he used for work and offered to allow agents to conduct a manual review of this computer. A manual review was conducted onsite, and no illicit

material was observed. Agents left their contact information with Clemence and advised that they would like Clemence's wife to contact them to arrange an interview. Clemence's wife, Elizabeth Clemence ("Elizabeth") contacted agents the following day and eventually made arrangements to be interviewed at her home on June 4, 2021.

17. On June 4, 2021 SA Mike Perella and I returned to 31 Adams Avenue in Rochester at approximately 10:44 a.m. to conduct a consensual interview of Elizabeth Clemence. Elizabeth disclosed that on May 18, 2019, she was printing church documents from a household computer and accessed a folder titled "Documents." She advised that the computer was a Dell laptop that belonged to her husband, but that they both used the computer. Within the "Documents" folder, she saw approximately 14,000 images and videos of what appeared to Elizabeth to depict child pornography. She described one file as two naked boys in a bathtub. In addition, Elizabeth advised that the filenames that she observed were consistent with child pornographic material. This occurred when they were living on Crow Hill Road in Rochester. Elizabeth advised that their internet connection at that home was secure and that nobody had the password.

18. Elizabeth advised that when she confronted Clemence about what she found on the computer, he stated he didn't know how it got there and suggested that their computer must have been hacked. Elizabeth explained that she and Clemence did not know what to do about the material she had located on their computer. They considered going to the police, but at the time they were exploring the possibility of fostering children and they were concerned about jeopardizing their ability to do so. As a result, they decided to wipe the hard drive themselves. They also changed the passwords to the computer and the wireless internet. Elizabeth recalled it

was possible that their neighbor, Kevin Mayfield, helped them change the password for the internet. They subsequently called an attorney the following Monday, and the attorney purportedly concurred that it was good they wiped the hard drive. Elizabeth advised that she and Clemence were very concerned about the incident when it occurred and that they talked about it with their pastor and several close friends.

19. Elizabeth advised that at the beginning of the pandemic, a couple that they were friends with from church, Drew and Sarah Lytle, were in need of a computer for Zoom meetings. Elizabeth and Clemence decided to give them their Dell laptop computer. Prior to giving the computer to the Lytles, Elizabeth and Clemence wiped the hard drive a second time. The Lytles gave the computer to their eldest son. Elizabeth advised that the Lytles live in Lebanon, Maine, and advised that after speaking with agents the week of May 26, 2021, Clemence did retrieve the Dell laptop computer from the Lytles.

20. Elizabeth advised that when she learned from Clemence that agents had been at their residence the previous week and learned the nature of their investigation, she checked all of the thumb drives in the house for the presence of child pornography. She did this without Clemence's knowledge. She advised that she did not locate anything that appeared to be child pornography. Elizabeth further disclosed that she and Clemence have an "open marriage" in the sense that they share access to each other's online accounts, including email, social media, financial accounts, etc. They also share access to the electronic devices in the home.

21. Elizabeth was asked whose name the internet service was in at their previous address on Elizabeth left the room to consult her records and returned with some paper files. Elizabeth was also asked about who paid the bills, took care of household

finances, etc., and Elizabeth stated that she did. Elizabeth was asked whether she recalled any unusual or suspicious purchases around the time of April or May 2019 when this activity occurred. She indicated she could not recall anything offhand, but asked if she could consult her records. She left the room and returned with a laptop computer, which she used to access her financial accounts and did not find anything noteworthy.

22. Elizabeth asked whether there was anything else that she should "look for," and SA Perella and I explained that we could not direct her to do any specific searching of Clemence's devices or accounts. However, we advised that there were certain applications and cloud storage accounts that are commonly encountered in these types of investigations. Elizabeth stated that Clemence did have a cloud storage account that she also had access to and stated that she was "on it right now." Elizabeth was advised that if she encountered anything concerning in the accounts to which she and her husband shared access, she should contact us. SA Perella and I left contact information with Elizabeth and departed the residence.

23. A short time later, while SA Perella and I were en route back to our office, I received a telephone call from Elizabeth Clemence. Elizabeth disclosed that while reviewing the contents of Clemence's Google Drive account, she observed approximately four videos that appeared to depict child pornography. She described one such video as two male children that were clothed and spanking each other. Another video appeared to depict two young boys, approximately 13 years old, performing oral sex on each other. She later described a third video in which it appeared that an adult male was engaged in anal penetration of a prepubescent boy that appeared to be approximately 10 years old. The boy was blindfolded and had something over his mouth.

24. Elizabeth advised that the cloud storage account is connected to her husband's Gmail account, which is @gmail.com, and that both the email address and password, both of which she has access to, are required to login to the Google Drive account. Elizabeth further stated that Clemence had access to his Gmail account on his cell phone.

25. Upon learning this information, SA Perella and I determined that we would return to the residence and secure it so that we could seek a search warrant. When we arrived back at the residence at approximately 2:50 pm, we observed a red Honda Civic with NH registration parked in the driveway. Clemence was seated in the driver's seat with the driver's door ajar and one foot out the door. Clemence appeared to have his cell phone in his hand. Upon parking our vehicle, Clemence exited his car, leaving the door ajar, and placed his cell phone on the front passenger seat. SA Perella observed the cell phone in plain view on the vehicle seat and noticed that the screen was illuminated and it appeared that a video was playing. SA Perella asked Clemence whether the cell phone on the seat was his, and Clemence confirmed that it was. SA Perella advised Clemence that agents would be securing the phone so that they could apply for a search warrant for its contents.

26. Clemence was extremely agitated and upset that agents had seized his phone. We explained that additional information had come to light since the interview with him the previous week. We further explained that Clemence was not under arrest and that he was free to leave. I advised Clemence of his rights, and Clemence advised that he would like to speak with a lawyer. I offered Clemence the use of my cell phone in order to allow Clemence to contact his attorney, but Clemence refused and insisted that he needed his own cell phone in order to get his attorney's contact information. Eventually, Clemence's wife provided a business card with their

attorney's phone number on it, but Clemence still declined to use agents' phones to call his attorney despite offers from multiple agents and local law enforcement officers who had arrived to help secure the residence. Clemence left the residence in his vehicle a short time later.

27. I reviewed two of the videos that Elizabeth previously described to me over the phone that appeared to Elizabeth to depict child pornography. Based on my training and experience, I agree that they appeared to depict child pornographic material. Elizabeth also described a concerning photograph of her 3 year old son that she found in Clemence's Google Drive account. She stated that her son was depicted naked from the waist down facing the wall. It appeared to have been taken in the basement of the home and depicted her son's buttocks. Elizabeth explained that Clemence is responsible for disciplining the children and stated that when he does so he takes them to a private area of the house. Elizabeth pointed out a wooden implement on a bureau in the children's bedroom that Clemence uses to discipline the children.

28. A search warrant was obtained for the residence and executed that same day. A preliminary review of devices and storage media seized from the residence revealed the presence of child pornography and child erotica on numerous devices, to include Clemence's Samsung cell phone, several thumb drives, and an SD card. Additional child pornography was also located in Clemence's Google Drive account. The images predominantly depicted male children, many of them prepubescent, and had a particular emphasis on bondage and spanking.

29. On June 7, 2021, a federal criminal complaint and arrest warrant was signed in the District of New Hampshire for Michael Clemence. Clemence was arrested without incident later that same day at Microtel Inn and Suites in Dover, New Hampshire. Another laptop computer was seized from his hotel room pursuant to a search warrant obtained subsequent to his arrest.

The remainder of Clemence's personal property was collected from the hotel room by Clemence's pastor at Clemence's request and returned along with Clemence's vehicle to Elizabeth.

30. On June 9, 2021, Elizabeth Clemence advised me that she found a blue DVD amongst Clemence's personal property inside his vehicle. Specifically, it was tucked in with various greeting cards that Clemence had saved that had been given to Clemence by Elizabeth. The disk is a blue Maxwell BD-R 25GB blu-ray disk. Elizabeth also advised that she found a thumb drive left on the desk in the office after the execution of the search warrant at their residence. She described it as a black Geek Squad thumb drive. Elizabeth expressed that she was unaware of the contents of these items, but that she did not wish for them to remain in her home.

31. On June 14, 2021, Elizabeth turned over the blu-ray disk and Geek Squad thumb drive to Danielle Ryan of DCYF. According to Ryan, she secured the items in her office. On June 30, 2021, HSI SA Michael Perella went to the DCYF Office and took custody of the items from Danielle Ryan. Both items are now secured at the HSI Office, 275 Chestnut Street, Suite 307, in Manchester, New Hampshire.

COMPUTERS, ELECTRONIC STORAGE AND FORENSIC ANALYSIS

32. As described above and in Attachment B, this application seeks permission to search and seize records that might be found on the SUBJECT DEVICES. I submit that there is probable cause to believe that such records may be found on the SUBJECT DEVICES, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Your Affiant is also aware, through training and experience, that digital storage devices have become interconnected, making it easy for even casual users of technology to transfer or copy images from one device to another, or to maintain duplicate copies on more than one device or storage medium. In fact, many devices such as smartphones can be set to automatically back up their contents to alternate storage facilities, such as laptop or desktop computers, another phone, photo-sharing websites, and cloud storage providers.

d. Your Affiant is aware that the contents of smart phones can be synched with or backed up to other digital devices in a variety of ways. Smartphones can be connected through cables to other devices, such as laptop computers, for data transfer. Smartphones can also connect to other devices and transfer photos or documents wirelessly through technology such as Bluetooth. Data can also be sent from the phone to an email account via the Internet, and

subsequently downloaded from the Internet to a different device (such as a tablet, game system, or computer) for storage. In addition, many smartphones utilize "cloud" storage. Cellular telephones can be set to automatically back up their contents to user accounts hosted on servers of various cloud storage providers. Users can also opt to perform a back-up manually, on an as-needed basis. Your Affiant is aware that some smartphones also back up their contents automatically to devices such as laptop computers. Additionally, cellular telephones can exchange data between two differing cellular communications devices and other types of electronic and media storage devices via Bluetooth or Wi-Fi, regardless of the type of operating system or platform being utilized to operate each of the electronic devices. In addition, media cards which contain many forms of data can be interchanged between multiple types of electronic devices, including but not limited to, different cellular telephones.

33. As set forth above, probable cause exists to believe that Clemence has received and/or possessed child pornography, and child pornography has been located on a variety of electronic devices and storage media owned and/or used by Clemence. Based upon my knowledge and experience in child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know that there are certain characteristics common to individuals involved in such crimes:

a. Those who distribute, transport, receive, or possess child pornography, or who attempt to commit these crimes may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Such individuals often times use these materials for their own sexual arousal and gratification.

b. Those who distribute, transport, receive, or possess child pornography, or who attempt to commit these crimes often possess and maintain copies of child pornography material, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. These individuals often retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years.

c. Those who distribute, transport, receive, or possess child pornography, or who attempt to commit these crimes often maintain their collections that are in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. They often maintain these collections for several years and keep them close by, usually at the individual's residence, to enable the collector to view the collection, which is valued highly.

d. Those who distribute, transport, receive, or possess child pornography, or who attempt to commit these crimes also may correspond with and/or meet others to share information and materials; they rarely destroy correspondence from other child pornography distributors/collectors; they conceal such correspondence as they do their sexually explicit material; and they often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

34. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the

purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on the SUBJECT DEVICES because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

b. Forensic evidence on a computer or storage medium can also indicate who has used or controlled the computer or storage medium. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, e-mail, e-mail address books, "chat," instant messaging logs, photographs, the presence or absence of malware, and correspondence (and the data associated with the foregoing, such as file creation and last-accessed dates) may be evidence of who used or controlled the computer or storage medium at a relevant time.

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it and when, it is sometimes necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

CONCLUSION

35. Based on the aforementioned factual information, I respectfully submit that there is probable cause to believe that evidence, fruits, and instrumentalities of the crime of possessing child pornography in violation of 18 U.S.C. § 2252(a)(4)(B) may be located on the SUBJECT DEVICES. I therefore seek a warrant to search the SUBJECT DEVICES described in Attachment A and to seize the items described in Attachment B.

/s/ Ronald Morin
Special Agent Ronald Morin
Department of Homeland Security
Homeland Security Investigations

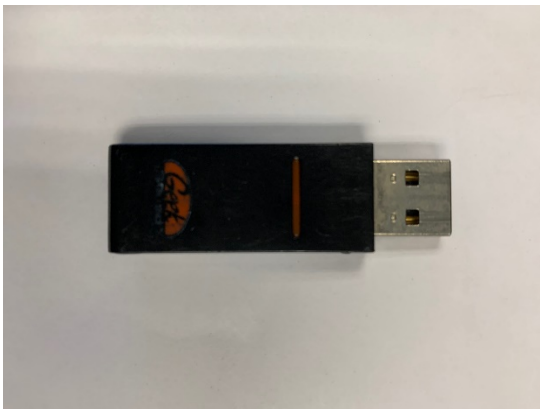
The affiant appeared before me by telephonic conference on this date pursuant to Fed. R. Crim. P. 4.1 and affirmed under oath the content of this affidavit and application.

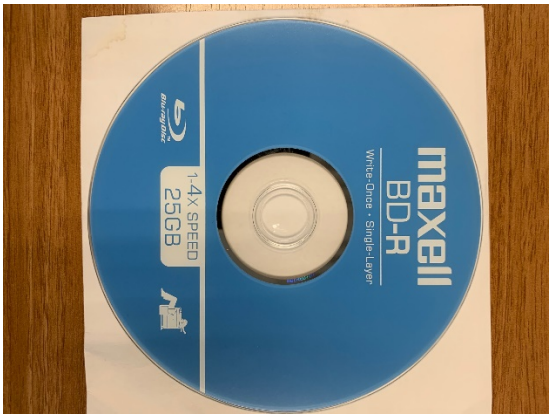
Date: July 9, 2021
Time: 5:36 PM, July 9, 2021

HONORABLE ANDREA K. JOHNSTONE
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

The premises to be searched includes one blue Maxwell BD-R 25GB blu-ray disk and one black Geek Squad thumb drive ("SUBJECT DEVICES"), now in the custody of HSI Manchester, 275 Chestnut St., Manchester, NH. The photographs below depict the SUBJECT DEVICES:





ATTACHMENT B

ITEMS TO BE SEIZED

The following materials, which constitute evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use or which is or has been used as the means of committing a criminal offense, namely violations of Title 18, United States Code, Sections 2252(a)(4)(B):

1. All records relating to violations of 18 U.S.C. §§ 2252(a)(4)(B) in any form wherever they may be stored or found on the SUBJECT DEVICES, including:

   a. records and visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256;

   b. records or information pertaining to an interest in child pornography;

   c. records or information pertaining to the possession, receipt, transportation, or distribution of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256;

   d. records or information of and relating to visual depictions that have been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct as defined in 18 U.S.C. § 2256, including the record or information used to create the visual depiction;

   e. photo-editing software and records or information relating to photo-editing software;

   f. records or information relating to the ownership, possession, or use of SUBJECT DEVICES.

2. For any computer, computer hard drive, or other physical object upon which electronic data can be recorded (hereinafter, "COMPUTER") that is called for by this warrant, or that might contain things otherwise called for by this warrant:

a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software;

d. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

e. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

f. evidence of the times the COMPUTER was used;

g. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

h. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

i. contextual information necessary to understand the evidence described in this attachment.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing, drawing, painting); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

As used above, the term "COMPUTER" includes but is not limited to any and all

computer equipment, including any electronic devices that are capable of collecting, analyzing, creating, displaying, converting, storing, concealing, or transmitting electronic, magnetic, optical, or similar computer impulses or data. These devices include but are not limited to any data-processing hardware (such as central processing units, memory typewriters, mobile "smart" telephones, tablets, and self-contained "laptop" or "notebook" computers); internal and peripheral storage devices (such as fixed disks, external hard disks, floppy disk drives and diskettes, thumb drives, flash drives, Micro SD cards, SD cards, CDs, DVDs, tape drives and tapes, optical storage devices, zip drives and zip disk media, and other memory storage devices); peripheral input/output devices (such as keyboards, printers, fax machines, digital cameras, scanners, plotters, video display monitors, and optical readers); and related communications devices (such as modems, routers, cables and connections, recording equipment, RAM or ROM units, acoustic couplers, automatic dialers, speed dialers, programmable telephone dialing or signaling devices, and electronic tone-generating devices); as well as any devices, mechanisms, or parts that can be used to restrict access to such hardware (such as physical keys and locks).